

CLAIMS

What is claimed is:

1. A method for deploying configuration instructions to security devices in order to implement a security policy in a network, the method comprising the computer-implemented steps of:
 - detecting that implementing a security policy will cause an address translation alteration in a packet communicated between a management source and a plurality of security devices for implementing the security policy on the network;
 - identifying, from among the plurality of security devices, one or more sets of security devices that have one or more configuration dependencies as a result of the address translation alteration if the security policy is implemented; and
 - sending one or more configuration instructions from the management source to each of the one or more sets of security devices using an order that is determined based on the one or more configuration dependencies, resulting in implementing the security policy on the network.

1 2. A method as recited in Claim 1, wherein sending configuration instructions from the
2 management source to the one or more sets of security devices includes sending
3 configuration instructions to multiple sets of security devices in parallel, wherein each of the
4 multiple sets of security devices includes one or more configuration dependencies.

5 3. A method as recited in Claim 2, wherein:

6 identifying one or more sets of security devices that would each have one or more
7 configuration dependencies as a result of the address translation alteration includes
8 identifying a first network path that interconnects the management source and a first
9 set of the one or more security devices in series, and a second network path that
10 interconnects the management source and a second set of the one or more security
11 devices in series; and
12 sending configuration instructions to multiple sets of security devices in parallel includes
13 sending configuration instructions to one or more security devices on the first network
14 path and on the second network path concurrently, and independently of one another,
15 using the order determined by the one or more configuration dependencies.

1 4. A method as recited in Claim 1, wherein:

2 identifying one or more sets of security devices that would each have one or more
3 configuration dependencies as a result of the address translation alteration includes
4 identifying a first network path that interconnects the management source and a first
5 set of the one or more security devices in series, and a second network path that
6 interconnects the management source and a second set of the one or more security
7 devices in series;

8 sending configuration instructions from the management source to each of the one or more
9 sets of security devices includes sending configuration instructions to one or more
10 security devices on the first network path and on the second network path in parallel;
11 and

12 sending configuration instructions to one or more security devices on the first network path
13 includes sending configuration instructions to at least some of the security devices on
14 the first network path sequentially, beginning with a first security device on the first
15 network path that is ordered to be a last one of the security devices on the first
16 network path to receive communications from the management source.

1 5. A method as recited in Claim 1, wherein:

2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a natural address translation between
5 the management source and one of the plurality of security devices.

1 6. The method as recited in Claim 1, wherein:
2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a static address translation between
5 the management source and one of the plurality of security devices.

1 7. A method as recited in Claim 1, wherein:
2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a tunneling translation between the
5 management source and one of the plurality of security devices

1 8. A method as recited in Claim 1, wherein:
2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a natural address translation;
5 identifying one or more sets of security devices that would each have one or more
6 configuration dependencies as a result of the address translation alteration includes
7 identifying a first network path that interconnects the management source and a first
8 set of the one or more security devices in series; and
9 sending configuration instructions from the management source to one or more sets of
10 security devices includes sending configuration instructions to at least some of the
11 security devices on the first network sequentially, beginning with a first security
12 device on the first network path that is ordered to be a last one of the security devices
13 on the first network path to receive communications from the management source.

1 9. A method as recited in Claim 1, wherein:
2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a static address translation on the first
5 network path; and
6 identifying one or more sets of security devices that would each have one or more
7 configuration dependencies as a result of the address translation alteration includes
8 identifying a first network path that interconnects the management source and a first
9 set of the one or more security devices in series;
10 sending configuration instructions from the management source to one or more sets of
11 security devices includes sending configuration instructions to one or more security
12 devices on the first network path using the order of either (i) sending configuration
13 instructions to each security device of the first network path that is ordered in series
14 between the management source and the static address translation before sending
15 configuration instructions from the management source to any of the other security
16 devices that are ordered in series after the static address translation, or (ii) sending
17 configuration instructions to all of the other security devices that are ordered in series
18 after the static address translation before sending configuration instructions from the
19 management source to each security device that is ordered between the management
20 source and the static address translation.

1 10. A method as recited in Claim 1, wherein:
2 detecting that implementing the security policy will cause an address translation alteration
3 between a management source and a plurality of security devices includes detecting
4 that implementing the security policy will cause a tunneling translation on the first
5 network path; and
6 identifying one or more sets of security devices that would each have one or more
7 configuration dependencies as a result of the address translation alteration includes
8 identifying a first network path that interconnects the management source and a first
9 set of the one or more security devices in series;
10 sending configuration instructions from the management source to one or more sets of
11 security devices includes sending configuration instructions to one or more security
12 devices on the first network path using the order of either (i) sending configuration
13 instructions to each security device of the first network path that is ordered in series
14 between the management source and the static address translation before sending
15 configuration instructions from the management source to any of the other security
16 devices that are ordered in series after the static translation, or (ii) sending
17 configuration instructions to all of the other security devices that are ordered in series
18 after the static translation before sending configuration instructions from the
19 management source to each security device that is ordered between the management
20 source and the tunneling translation.

1 11. A method for deploying configuration instructions to security devices in order to
2 implement a security policy in a network, the method comprising the computer-implemented
3 steps of:

4 detecting that the security policy creates a change of one or more configuration
5 dependencies as compared with an existing security policy, each configuration
6 dependency corresponding to at least a first security device having to be
7 configured before a second security device is configured in order for the first
8 security device to receive its configuration instructions for implementing the
9 security policy from a management source; and
10 deploying configuration instructions to one or more security devices to implement the
11 security policy according to an order determined by the one or more
12 configuration dependencies.

1 12. A method as recited in Claim 11, wherein deploying configuration instructions
2 includes deploying, for a network path containing at least a first configuration dependency of
3 the one or more configuration dependencies, configuration instructions to a first security
4 device of the first configuration dependency before deploying configuration instructions to a
5 second security device of the first configuration dependency, wherein the first security device
6 has to be configured before the second security device in order for the first security device to
7 receive its configuration instructions for implementing the security policy from the
8 management source.

1 13. A method as recited in Claim 11, further comprising creating a schedule to implement
2 the security policy to account for the change in the one or more configuration dependencies,
3 and wherein deploying configuration instructions to one or more security devices includes
4 using the schedule to deploy the configuration instructions.

1 14. A method as recited in Claim 13, wherein deploying configuration instructions
2 includes deploying in parallel the configuration instructions to each of the first security
3 devices in the one or more configuration dependencies.

1 15. A method as recited in Claim 11, wherein detecting that the security policy creates a
2 change of one or more configuration dependencies from an existing security policy includes
3 detecting the addition, deletion or modification of an address translation in a network path
4 between the one or more security devices and the policy manager.

1 16. A method as recited in Claim 14, further comprising detecting the addition, deletion
2 or modification of the address translation selected from an address translation type consisting
3 of a natural address translation type, a reverse address translation type, and a tunnel
4 translation.

5 17. A computer-readable medium for deploying configuration instructions to security
6 devices in order to implement a security policy in a network, the computer-readable medium
7 carrying instructions for implementing the steps of:

8 detecting that implementing a security policy will cause an address translation
9 alteration in a packet communicated between a management source and a
10 plurality of security devices for implementing the security policy on the
11 network;
12 identifying, from among the plurality of security devices, one or more sets of security
13 devices that have one or more configuration dependencies as a result of the
14 address translation alteration if the security device is implemented; and
15 sending one or more configuration instructions from the management source to each
16 of the one or more sets of security devices using an order that is determined
17 based on the one or more configuration dependencies, resulting in
18 implementing the security policy on the network.

1 18. A computer-readable medium as recited in Claim 17, wherein instructions for sending
2 one or more configuration instructions from the management source to each of the one or
3 more sets of security devices include instructions for sending configuration instructions to
4 multiple sets of security devices in parallel, wherein each of the multiple sets of security
5 devices includes one or more configuration dependencies.

1 19. A computer-readable medium as recited in Claim 18, wherein:
2 instructions for identifying one or more sets of security devices that would each have one or
3 more configuration dependencies as a result of the address translation alteration
4 include instructions for identifying a first network path that interconnects the
5 management source and a first set of the one or more security devices in series, and a
6 second network path that interconnects the management source and a second set of
7 the one or more security devices in series; and
8 instructions for sending one or more configuration instructions to multiple sets of security
9 devices in parallel include instructions for sending configuration instructions to one or
10 more security devices on the first network path and on the second network path
11 concurrently, and independently of one another.

1 20. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for identifying one or more sets of security devices that would each have one or
3 more configuration dependencies as a result of the address translation alteration
4 include instructions for identifying a first network path that interconnects the
5 management source and a first set of the one or more security devices in series, and a
6 second network path that interconnects the management source and a second set of
7 the one or more security devices in series;
8 instructions for sending one or more configuration instructions from the management source
9 to each of the one or more sets of security devices I include sending configuration
10 instructions to one or more security devices on the first network path and on the
11 second network path in parallel, including for sending configuration instructions to at
12 least some of the security devices on the first network path sequentially, beginning
13 with a first security device on the first network path that is ordered to be a last one of
14 the security devices on the first network path to receive communications from the
15 management source.

1 21. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 natural address translation between the management source and one of the plurality of
6 security devices.

1 22. The computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 static address translation between the management source and one of the plurality of
6 security devices.

1 23. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 tunneling translation between the management source and one of the plurality of
6 security devices

1 24. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 natural address translation;
6 instructions for identifying one or more sets of security devices that would each have one or
7 more configuration dependencies as a result of the address translation alteration
8 include instructions for identifying a first network path that interconnects the
9 management source and a first set of the one or more security devices in series; and
10 instructions for sending one or more configuration instructions from the management source
11 to one or more sets of security devices include instructions for sending configuration
12 instructions to at least some of the security devices on the first network sequentially,
13 beginning with a first security device on the first network path that is ordered to be a
14 last one of the security devices on the first network path to receive communications
15 from the management source.

1 25. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 static address translation on the first network path;
6 instructions for identifying one or more sets of security devices that would each have one or
7 more configuration dependencies as a result of the address translation alteration
8 include instructions for identifying a first network path that interconnects the
9 management source and a first set of the one or more security devices in series; and
10 instructions for sending configuration instructions from the management source to one or
11 more sets of security devices include instructions for sending configuration
12 instructions to one or more security devices on the first network path using the order
13 of either (i) sending configuration instructions to each security device of the first
14 network path that is ordered in series between the management source and the static
15 address translation before sending configuration instructions from the management
16 source to any of the other security devices that are ordered in series after the static
17 address translation, or (ii) sending configuration instructions to all of the other
18 security devices that are ordered in series after the static address translation before
19 sending configuration instructions from the management source to each security
20 device that is ordered between the management source and the static address
21 translation.

1 26. A computer-readable medium as recited in Claim 17, wherein:
2 instructions for detecting that implementing the security policy will cause an address
3 translation alteration between a management source and a plurality of security devices
4 include instructions for detecting that implementing the security policy will cause a
5 tunneling translation on the first network path;
6 instructions for identifying one or more sets of security devices that would each have one or
7 more configuration dependencies as a result of the address translation alteration
8 include instructions for identifying a first network path that interconnects the
9 management source and a first set of the one or more security devices in series; and
10 instructions for configuration instructions from the management source to one or more sets of
11 security devices include instructions for sending configuration instructions to one or
12 more security devices on the first network path using the order of either (i) sending
13 configuration instructions to each security device of the first network path that is
14 ordered in series between the management source and the static address translation
15 before sending configuration instructions from the management source to any of the
16 other security devices that are ordered in series after the static translation, or (ii)
17 sending configuration instructions to all of the other security devices that are ordered
18 in series after the static translation before sending configuration instructions from the
19 management source to each security device that is ordered between the management
20 source and the tunneling translation.

1 27. A computer system for deploying configuration instructions to security devices in
2 order to implement a security policy in a network, the computer system comprising:

3 means for detecting that implementing the security policy will cause an
4 address translation alteration between a management source and a
5 plurality of security devices for implementing the security device on
6 the network;

7 means for identifying, from the plurality of security devices, one or more sets
8 of security devices that would each have one or more configuration
9 dependencies as a result of the address translation alteration; and

10 means for sending configuration instructions from the management source to
11 each of the one or more sets of security devices in order to implement
12 the security policy.

1 28. A management device for deploying configuration instructions to a plurality of
2 security devices in order to implement a security policy on a network, the management
3 device comprising:

4 a processor configured to:

5 detect that implementing the security policy will cause an address translation
6 alteration between a management source and a plurality of security
7 devices for implementing the security device on the network;

8 identify, from the plurality of security devices, one or more sets of security
9 devices that would each have one or more configuration dependencies
10 as a result of the address translation alteration; and

11 send configuration instructions from the management source to each of the
12 one or more sets of security devices using an order that is determined
13 by the one or more configuration dependencies, so as to implement the
14 security policy on the network.